UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/781,304	02/13/2001	Francisco Andeyro Garcia	202408US2	9121

22850 7590 08/17/2004

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 08/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/781,304	GARCIA, FRANCISCO ANDEYRO	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 February 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

2. The effective filing date for the subject matter defined in the pending claims in this application is 02/13/2001.

Specification

3. The disclosure is objected to because of the following informalities:

4. The first sentence on the first paragraph has spelling error. It should be "secret key" instead of "secete key". See 37 CFR 1.71.

Appropriate correction is required.

Claim Objections

5. Claim 15 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependency on claim 10 or claim 14, where the claim 14 should not serve as a basis for another multiple dependent claim which has a multiple dependency on claim 10 or claims 11, 12, or 13. See MPEP § 608.01(n).

6. Same objections to claims 17 and 31.

7. Any other claims not addressed by virtue of their dependency should also be corrected.

8. Claim 31 is objected to because of the following informalities: "programme" should be "programmed". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1, and 26 – 28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

10. Regarding claims 1 and 26 – 28, the phrase "such as" (or "similar to") renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. This includes "such as Bressenham algorithm", "similar to Bressenham algorithm" and "such as a Logic Xor". See MPEP § 2173.05(d). Appropriate correction is required

11. All the claims not addressed are objected by virtue of dependency on the claims 1 and 26 – 28.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1 – 14, 16, 17, 21 – 23 and 26 – 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rhoads-1996 (Patent Number: 6122403), hereinafter referred to as Rhoads-1996, in view of Rhoads-2000 (Patent Number: US 6424725 B1), hereinafter referred to as Rhoads-2000.

13. As per claim 1, Rhoads-1996 teaches a method based on an algorithm capable of being graphically implemented to be used for the generation or filtering of data sequences and cryptographic applications comprising the following stages:

a. Defining a cell array distribution with a computer, referenced to a system of coordinates in a vector bidimensional space, provided that the cells in question are capable of adopting two states (Rhoads-1996: see for example, Figure 21B, Figure 42 and Column 98 Line 24 – 26 and Column 97 Line 37 – 38).

b. definition of a first area within that bidimensional vector space, bordered by a first contour, using part of the said cells to define the successive points of the first contour and including a certain number of those cells in this first area (Rhoads-1996: see for example, Figure 21B, Figure 42, Column 53 Line 55 – 62, Column 54 Line 18 – 22 and Column 58 Line 33 – 48: The bump taught by Rhoads-1996 (or SUB-BLOCK shown in Figure 42) is equivalent to one type of first contours);

c. definition of a second area in that bidimensional space bordered by a second contour using part of the cells to define the subsequent points of the same; this second

area contains the first area (Rhoads-1996: see for example, Figure 21B, Figure 42, Column 101 Line 25 – 32, Column 53 Line 55 – 62, Column 54 Line 18 – 22 and Column 58 Line 33 – 48);

14. Rhoads-1996 teaches x-y Cartesian coordinates (Rhoads-1996: see for example, Column 98 Line 24 – 26).

15. Rhoads-1996 does not teach choosing a cell as the pole, and plot a set of lines from the pole of that cell, and repeat the process, up to a given number of cells which define the second contour, covering all or part of that contour until the first area has been fully swept, using for each line the cells determined by a plotting device such as a Bressenham algorithm;

16. Rhoads-2000 teaches choosing a cell as the pole, and plot a set of lines from the pole of that cell, and repeat the process, up to a given number of cells which define the second contour, covering all or part of that contour until the first area has been fully swept (Rhoads-2000: see for example, Column 7 Line 44 – 50, Figure 2 and Column 8 Line 59 – 63).

17. However, It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Rhoads-2000 within the system of Rhoads-1996 because (1) Rhoads-1996 teaches x-y Cartesian coordinates (Rhoads-1996: see for example, Column 98 Line 24 – 26), and (2) Rhoads-2000 further teaches transforming sweeping through the transformed image data along a line at angle θ and translating the Cartesian coordinates into Polar coordinate system (Rhoads-2000: see for example, Column 7 Line 44 – 50, Figure 2). As a result, sweeping a line 360 degree

would cover an entire given target image (3) Rhoads-1996 teaches group of pixels is termed bit cells. According to well-known Bressenham algorithm, a group of pixels (Integer-number domain) can be selected (and best-fit) for a given points on the line (Real-number domain) (4) Rhoads-1996 also teaches a certain pixel (or sample point / location) is selected and assigned to some predetermined security sensitive data which is then added into the original images (Rhoads-1996: see for example, Column 35 Line 18 – 20, Column 35 Line 31 – 33 and Column 35 Line 63 – 66). This pre-defined location can be considered as equivalent to the predefined "pole" location.

18. Rhoads-1996 as modified further teaches:

e. perform an operation on the contents of each of the cells used when plotting each of the lines of the set and included in that first contour, thereby transforming their state, such as a Logic Xor, each time the cell in question is found in one of the lines of the set (Rhoads-1996: see for example, Column 28 Line 43 – 47, Column 58 Line 57, Column 35 Line 66 – 67 and Column 36 Line 1 – 4: Rhoads-1996 teaches encryption on the data content and XOR function is evidently one of the well-known and widely used ciphering functions).

19. As per claims 26 and 27, claims 26 and 27 do not further teach over claim 1 because Rhoads-1996 discloses the coordinate (and axis) can be extended to three dimensions (Rhoads-1996: see for example, Column 98 Line 15 – 19).

20. As per claim 28, claim 28 does not further teach over claim 1 because Rhoads-1996 discloses the coordinate (and axis) can be simplified to one-dimension case (Rhoads-1996: see for example, Column 52 Line 35 – 37).

21. As per claim 2, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 1). Rhoads-1996 as modified further teaches a method pursuant to the foregoing claim, best described because the bidimensional space in question is materialized in a computer screen and the array distribution of cells is defined by a specific resolution of the screen, which may be selected, and each cell is considered as a pixel or basic element of an image or its analytical representation (Rhoads-1996: see for example, Column 97 Line 32).

22. As per claim 3, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 1 or 2). Rhoads-1996 as modified further teaches characterized in that the second contour matches with the first contour (Rhoads-1996: see for example, Column 101 Line 25 – 32).

23. As per claim 4, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 1 or 2). Rhoads-1996 as modified further teaches characterized in that the second contour and the first contour are rectangular and its sides are parallel (Rhoads-1996: see for example, Figure 21B and a square is also a rectangular).

24. As per claim 5, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 2). Rhoads-1996 as modified further teaches characterized in that the second contour is the border of the graphic screen or an analytical representation of the same (Rhoads-1996: see for example, Column 58 Line 37).

25. As per claim 6, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 1). Rhoads-1996 as modified further teaches characterized

in that the pole is located within the area enclosed by the second contour (Rhoads-1996: see for example, Column 52 Line 46).

26. As per claim 7, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 6). Rhoads-1996 as modified further teaches characterized in that the pole in question is located in a cell next to one of the two contours (Rhoads-1996: see for example, Column 52 Line 46).

27. As per claim 8, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 1). Rhoads-1996 as modified further teaches characterized in that the second contour is unregularized and the cells of the same are obtained by means of a Pseudo-Noise Sequence Generator (PNSG), so that the distance from the cells within that second contour to their corresponding pole is dependent on the output of the Pseudo-Noise Sequence Generator (Rhoads-1996: see for example, Column 3 Line 41 – 42, Column 97 Line 50 – 58 and Column 97 Line 61 – 62: the well-known randomization technique introduces significant complexity, making cryptographic analysis far more difficult).

28. As per claim 9, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 1). Rhoads-1996 as modified further teaches characterized in that the distance from the pole to the origin of the reference coordinates is obtained by means of Pseudo-Noise Sequence Generator (PNSG), so that the distance in question is dependent on the output of the Pseudo-Noise Sequence Generator (Rhoads-1996: see for example, Column 51 Line 33 – 35 and Column 51 Line 41: the

well-known randomization technique introduces significant complexity, making cryptographic analysis far more difficult).

29. As per claim 10, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 1). Rhoads-1996 as modified further teaches characterized in that it likewise includes a stage d1) prior to e) which consists in assigning the successive values of a data block with a certain length, or undetermined, to be encrypted or filtered, associating them in a pre-arranged manner to the cells of the said array delimited by the first contour and in that the extraction of data obtained by the application of this method is likewise carried out by means of an appropriate association to the cells in question in a pre-established manner (Rhoads-1996: see for example, Column 103 Line 51 – 60, Column 26 Line 52 and Column 26 Line 44).

30. As per claim 11, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 10). Rhoads-1996 as modified further teaches characterized in that the prearranged association of data to the cells in question is made in order, row by row (Rhoads-1996: see for example, Column 103 Line 51 – 60, Column 26 Line 52 and Column 26 Line 44).

31. As per claim 12, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 10). Rhoads-1996 as modified further teaches characterized in that the prearranged association of data to the cells in question is made in order, column by column (Rhoads-1996: see for example, Column 103 Line 51 – 60, Column 26 Line 52 and Column 26 Line 44).

32. As per claim 13, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 10). Rhoads-1996 as modified further teaches characterized in that the foregoing prearranged association of data to the cells is made in radial order starting from a pole with the precaution of not overlapping data so that such data only occupies positions not yet occupied in the array of cells to be filled in (Rhoads-1996: see for example, Column 103 Line 51 – 60, Column 26 Line 52 and Column 26 Line 44) & (Rhoads-2000: see for example, Column 7 Line 44 – 50, Figure 2).

33. As per claim 14, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 10). Rhoads-1996 as modified further teaches characterized in that the foregoing prearranged association of data to the cells is undertaken pursuant to any of the claims 11 to 13, and its extraction or reading is made according to any of the procedures set out in claims 11 to 13 (Rhoads-1996: see for example, Column 103 Line 51 – 60, Column 26 Line 52 and Column 26 Line 44).

34. As per claim 16, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 10). Rhoads-1996 as modified further teaches characterized in that stages a), b), c), d), d1 and e) are repeated a certain number of times at will, and each time any of the following variants may be applied: choice of different poles; change of contour size or form, or relative distance and position between the first and second contours in question; and undertaking a specific number of complete or incomplete rotations of the second contour, on plotting the set of lines

originating from the pole and based on the cells from the second contour (Rhoads-1996: see for example, Column 34 Line 15 – 18).

35. As per claim 17, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 10 – 16). Rhoads-1996 as modified further teaches Method for the encryption and decryption of messages relayed between a first and second station, or between multiple stations, consisting in variable length binary data blocks, and using the same graphic or analytic algorithm both for encryption and decryption as set out in claims 10 to 16, the data being introduced in an array delimited by the first contour and because the operation, made on the contents of a cell each time this cell of the first contour is used to plot a line of the set, makes use of the value stored in such cell and its corresponding value in a pseudo-random linear sequence generator, and the correlation is established pursuant to a specific order in the data array of the first contour, and if the data introduced, completely fills the array in question, the additional data is assigned, defining new pairs of first and second contours, being the first of these a new array for the loading of plaindata. And so on, until plaindata is off (Rhoads-1996: see for example, Column 193 Line 45).

36. As per claim 21 and 23, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 17 and 21 respectively). Rhoads-1996 as modified further teaches characterized in that the cell content is any type of digital data subject to being handled, treated or stored individually as a bit, byte, nibble, word, double word, and the number of possible states of the cells includes all the possibilities which are

specific to the nature of the type of data in question, or at least some of them (Rhoads-1996: see for example, Column 34 Line 53 – 58).

37. As per claim 22, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 21). Rhoads-1996 as modified further teaches characterised in that the contents of each cell are data bits and those cells are subject to undergoing at least two states (Rhoads-1996: see for example, Column 97 Line 38).

38. As per claim 29, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 26 or 27). Rhoads-1996 as modified further teaches characterized in that apart from including a preliminary phase d1) before e) which consists in assigning the subsequent values of a data block whether of definite or indeterminate length, to be encrypted, or filtered, associating them in a prearranged manner to the cells of that array delimited by the first encircling perimeter in question, and in that the operation to extract data following the application of this method is also conducted by means of a prearranged association, as may be appropriate (Rhoads-1996: see for example, Line Column 103 Line 51 – 60, Column 26 Line 52, Column 26 Line 44 and Column 98 Line 20).

39. As per claim 30, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 28). Rhoads-1996 as modified further teaches characterized in that it likewise includes a preliminary phase d1) prior to e) which consists in assigning the subsequent values of a data block whether of definite or indeterminate length, to be encrypted, or filtered, associating them in a prearranged manner to the cells of that array delimited by the first segment, and in that the operation

of data extraction following the application of this method is also conducted by means of a prearranged association, as may be appropriate (Rhoads-1996: see for example, Line Column 103 Line 51 – 60, Column 26 Line 52, Column 26 Line 44 and Column 98 Line 20).

40. As per claim 31, Rhoads-1996 as modified teaches the claimed invention as described above (see claims 1 – 3, 6 – 14, and 16 – 28). Rhoads-1996 as modified further teaches a computer programmed directly loaded in the memory of a computer including parts of the programming code to perform stages set out in claims 1 to 3, 6 to 14, and 16 to 28 when the said programmed is executed in that computer (Rhoads-1996: see for example, Figure 4).

41. Claims 15, 18 – 20, 24 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rhoads-1996 (Patent Number: 6122403), hereinafter referred to as Rhoads-1996, in view of Rhoads-2000 (Patent Number: US 6424725 B1), hereinafter referred to as Rhoads-2000, and in view of Koopman (Patent Number: 5363448), hereinafter referred to as Koopman.

42. As per claim 15, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 10 – 14). Rhoads-1996 as modified does not teach characterized in that the data block to be ciphered is made of a sequence stream generated by a Linear Feedback Shifted Register (LFSR).

43. Koopman teaches characterized in that the data block to be ciphered is made of a sequence stream generated by a Linear Feedback Shifted Register (LFSR). (Koopman: see for example, Column 4 Line 68).

44. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Koopman within the system of Rhoads-1996 as modified because Koopman teaches the LFSR technique introduces significant complexity, making cryptographic analysis far more difficult and thereby enhances the security.

45. As per claim 18, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 17). Rhoads-1996 as modified teaches characterized in that the values of the pseudo-randomly generated linear sequence, for example, by a linear feedback shifted register (LFSR) of n degree, are filtered by any of the methods provided under claims 10 to 16, operating as a non-linear filtering method (Rhoads-1996: see for example, Column 58 Line 52 – 60) & (Koopman: see for example, see for example, Column 4 Line 68).

46. As per claim 19 and 24, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 17 and 18 respectively). Rhoads-1996 as modified teaches characterised in that it includes a secret key, randomly generated to be exchanged by means of a secure server between the sender(s) and recipient(s), the said key being the same for the encryption and decryption process, the contents of such key comprise the definition of the Linear Feedback Shifted Register, as well as the coordinates of the pole, the array size, the distance from the first contour to the second

one, and any other parameter which may be required for any of the specific implementations foreseen under any of the methods set forth in claims 10 to 16 (Rhoads-1996: see for example, Column 51 Line 24 – 41) & (Koopman: see for example, see for example, Column 4 Line 68).

47. As per claim 20, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 19). Rhoads-1996 as modified teaches characterized in that the Linear Feedback Shifted Register (LFSR), is defined by a binary coefficient polynomial and a seed or initial state of the LFSR apt for the generation of a periodic sequence (Rhoads-1996: see for example, Column 58 Line 52 – 60) & (Koopman: see for example, see for example, Column 6 Line 25 – 30).

48. As per claim 25, Rhoads-1996 as modified teaches the claimed invention as described above (see claim 24). Rhoads-1996 as modified teaches characterized in that the said (LFSR) includes a binary seed of degree 63 and a primitive polynomial of degree 63 (Koopman: see for example, see for example, Column 6 Line 25 – 30: Higher degree of polynomial just means more security).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100